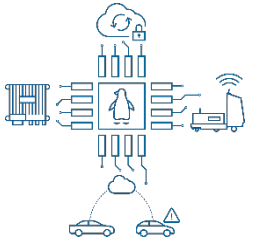
OPEN SESAME!

WHY FUNCTIONAL SAFETY IS THE MASTER KEY TO OPEN THE DOOR FOR LINUX INTO AUTOMOTIVE SYSTEMS

Authors: Nico Peper, Jan-Christian Arnold, Hans-Leo Ross

Agenda



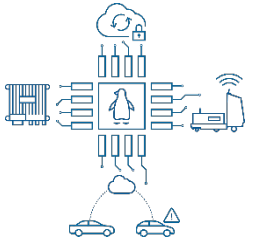
1. Why Automotive Software is special
2. Short introduction to Automotive Safety
3. Introducing an example: Linux powering Vehicle to Infrastructure communication (V2X)
4. Implementing ASIL B on a V2X traffic light
5. Safety relevant open questions in a V2X context
6. Conclusion

WHY AUTOMOTIVE SOFTWARE IS SPECIAL & SHORT INTRODUCTION TO AUTOMOTIVE SAFETY

BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Why Automotive Software is special



Open source

- Most automotive systems are powered purely by closed source software
- Licence obligations, like given in GPL V3, are often a blocking point

LTS

- Automotive base requirement is a 15 year product live cycle

Process

- To achieve high volume low cost scalability process orientation is the automotive fundamental approach

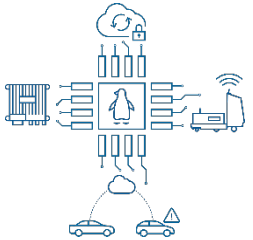
Legislative

- Safety -> Functional safety -> ISO26262

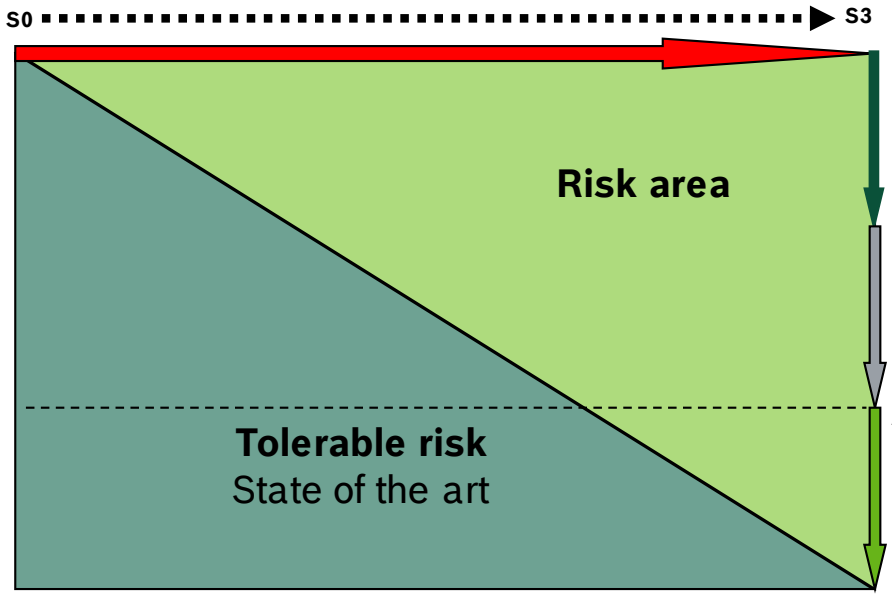
BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Short introduction to automotive safety



Potential damage caused by the operation of the vehicle or additional functions (S = extent of damage)



E4

Probability of hazardous situation
- **E = probability.**
  (Situation x risk)

E1
C3

Aversion of dangerous events
- **C =Controllability**
- Measures of other technology
- External measures
- Driver warning, if regulated by law

C0
ASIL A

Safety Integrity Measures according ISO 26262

only risk due malfunctions of EE system considered!

ASIL D

Area of risk and tolerable risk (Source: various different publications)

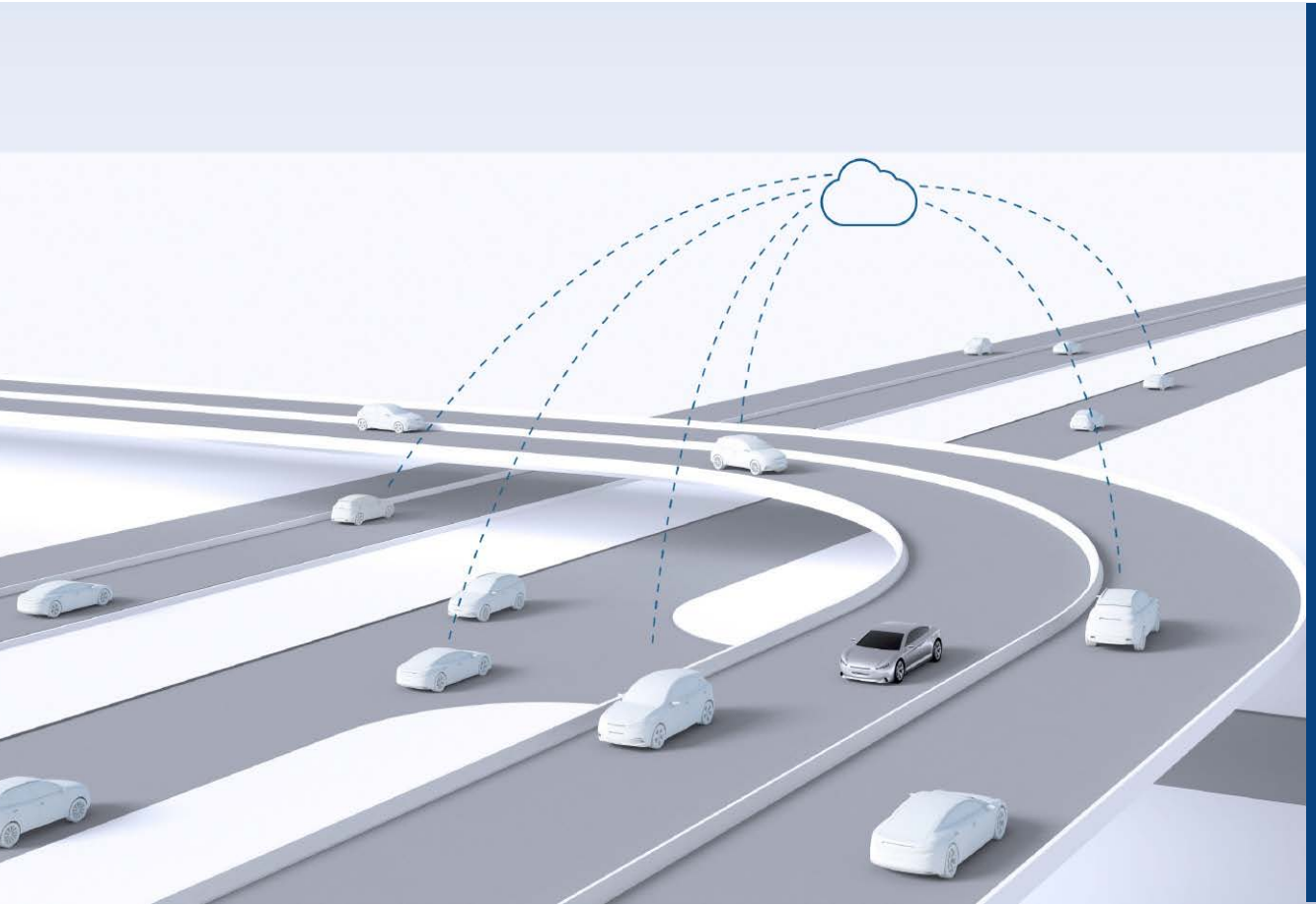
BOSCH

INTRODUCING AN EXAMPLE: LINUX POWERING VEHICLE TO INFRASTRUCTURE COMMUNICATION (V2X)

BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Linux powering V2X communication



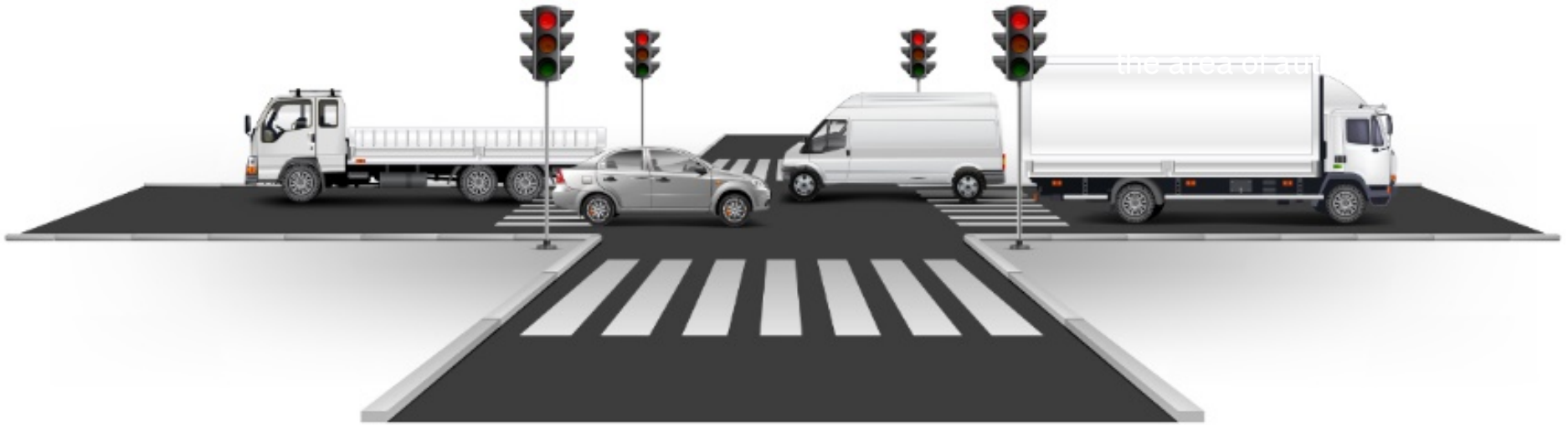
- V2X enables the direct communication between cars (V2V) and infrastructure (V2X)
- It's an enabler for advanced driving assistance and autonomous driving functions
- US government is actively pushing V2X systems by legislation. Standard will be released soon
- Todays V2X communication stacks are POSIX based implementations
- Systems need to handle complex and non-deterministic systems and algorithms (Fuzzy, neuronal networks etc.)

→ Linux will make a clear push to autonomous driving systems by operating V2X

BOSCH

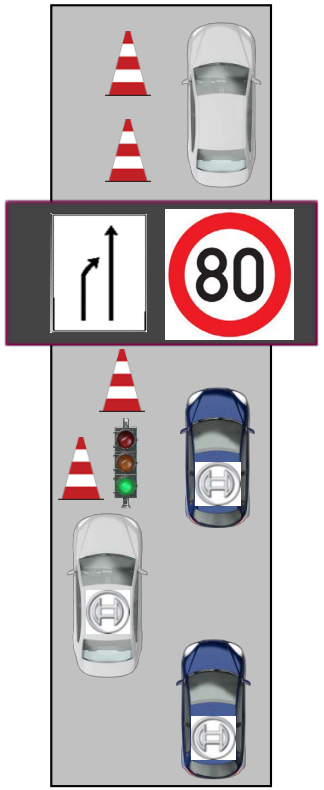
Open Sesame! Functional Safety for Linux in Automotive

Linux powering V2X communication

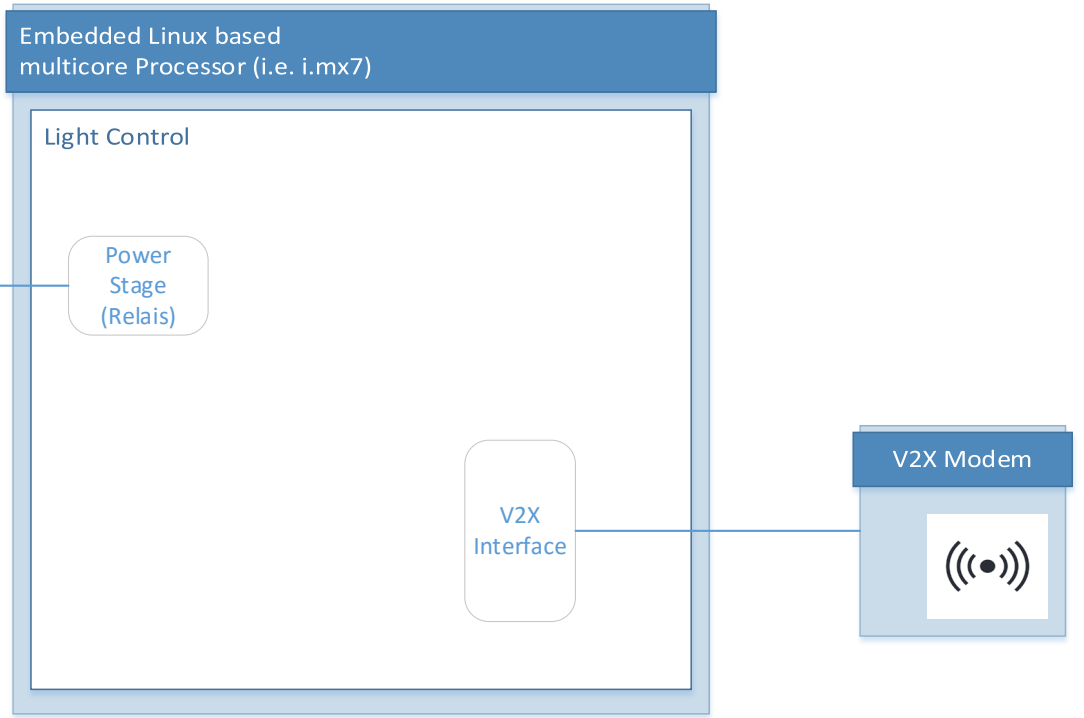


Open Sesame! Functional Safety for Linux in Automotive

Linux powering V2Xcommunication



System level



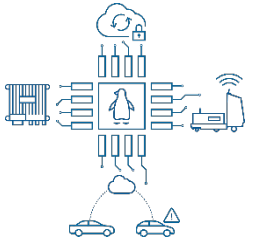
Base layout for connected traffic light control system

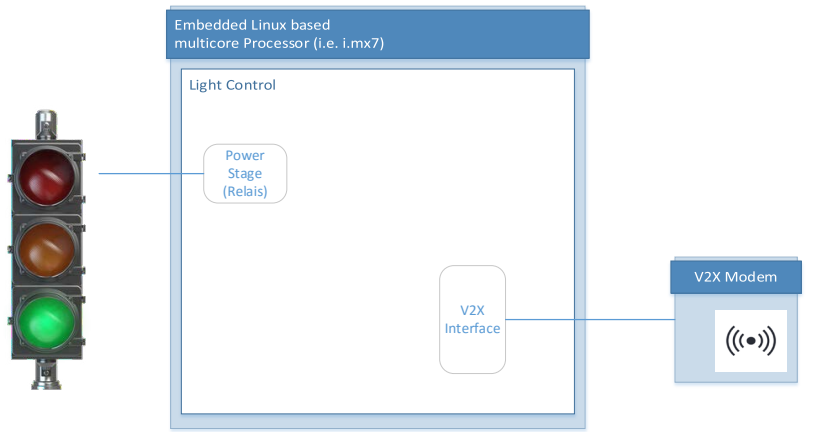
Bosch Engineering | Nico Peper, Jan-Christian Arnold, Hans-Leo Ross | October 2017

BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Linux powering V2X communication



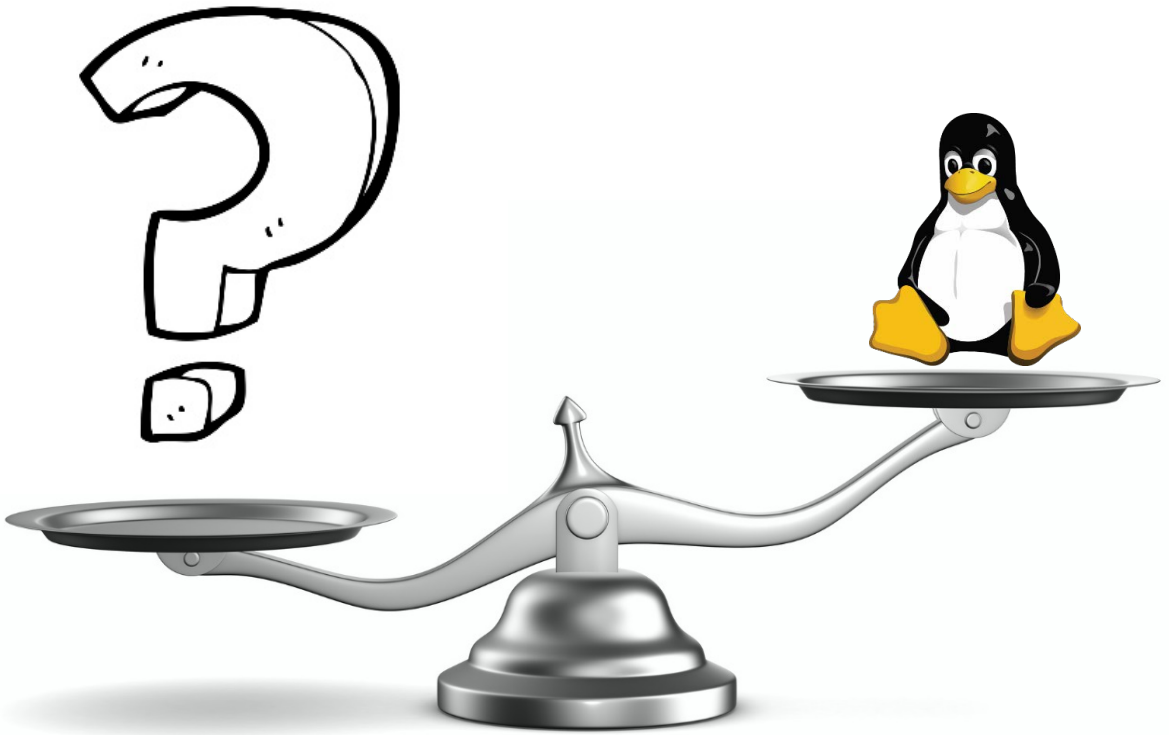


Bosch Engineering | Nico Peper, Jan-Christian Arnold, Hans-Leo Ross | October 2017

BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Linux powering V2X communication

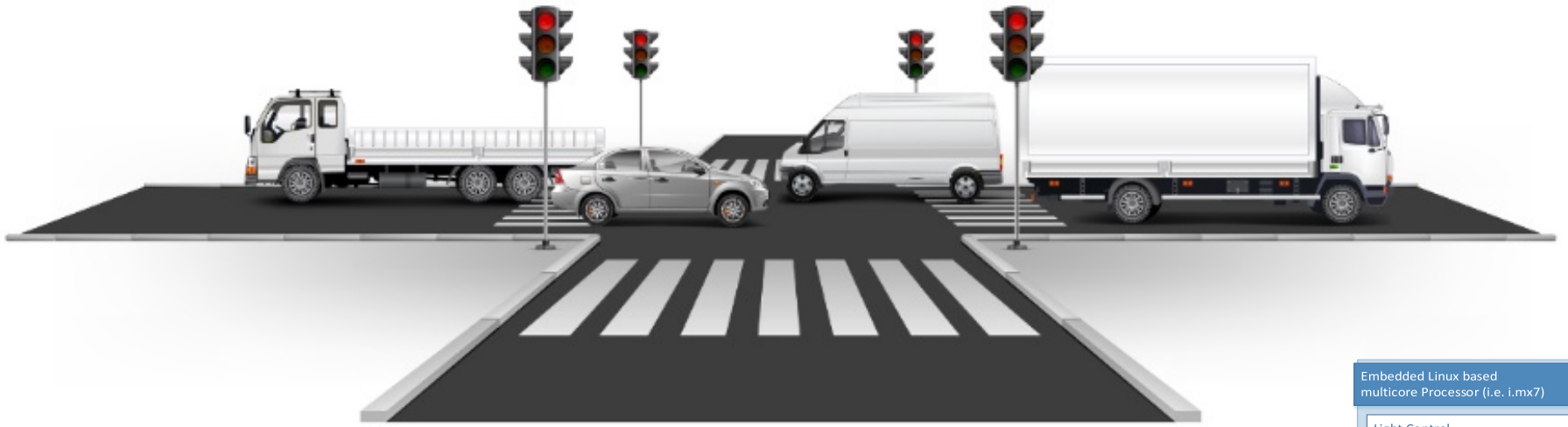


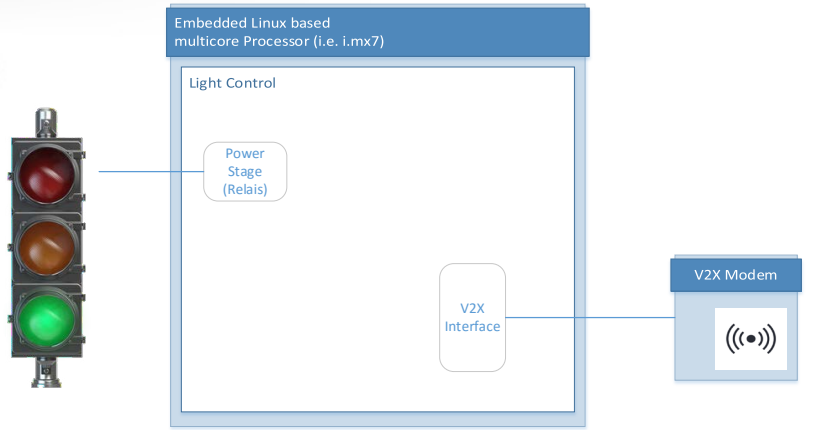
IMPLEMENTING ASIL B ON A V2X TRAFFIC LIGHT

BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on a V2X traffic light



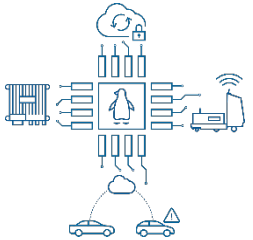


Bosch Engineering | Nico Peper, Jan-Christian Arnold, Hans-Leo Ross | October 2017

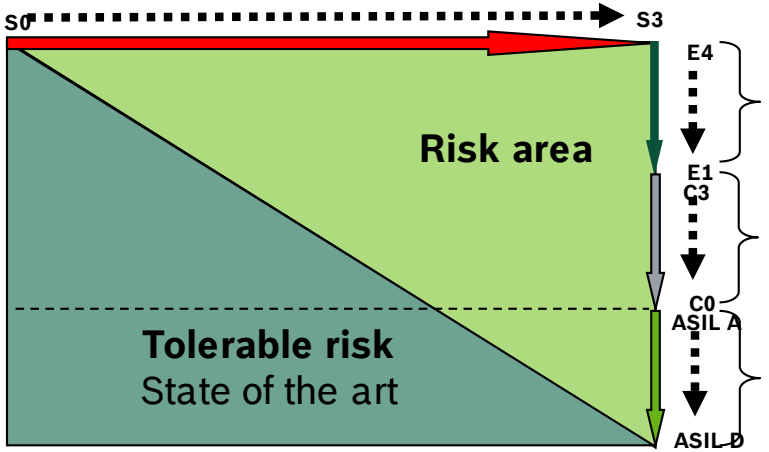
BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on a V2X traffic light

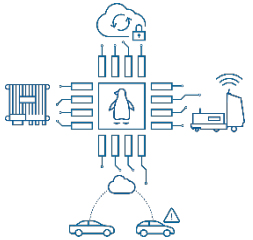


- In contrast trying to reach ASIL B by handling the system based on processes a system within system functionality view within given context needs to be introduced
- Hazard risks are safely to be reduced by determine their severity (expected loss) and frequency / probability
- The system functionality must be reliable and in case of system errors a sufficient safety level (safe state) needs to be achieved
- State of the art safety measures are needed to assure safe operation of vehicles!



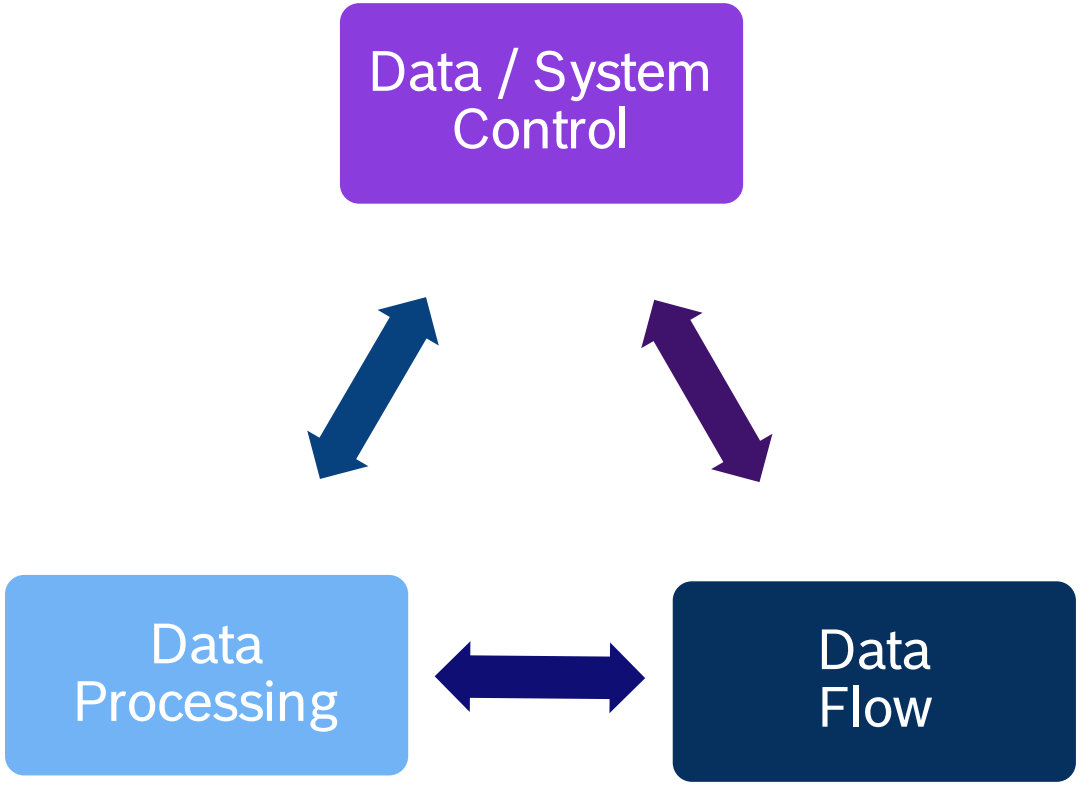
$$R = \sum_{\text{For all accidents}} (\text{probability of the accident occurring}) \times (\text{expected loss in case of the accident})$$

Open Sesame! Functional Safety for Linux in Automotive
Implementing ASIL B on a V2X traffic light



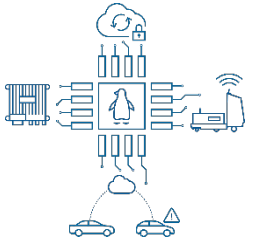
- An IT system may be represented by it's basic functionalities:
  - Data and system control
  - Data flow
  - Data processing

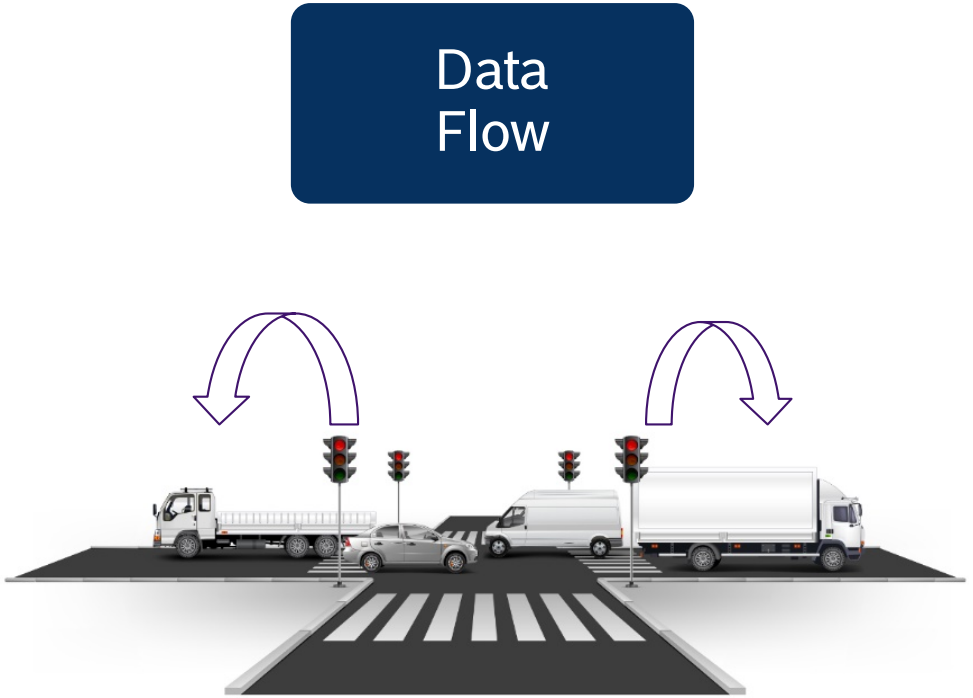
- To achieve safety integrity of the overall system these basic functionalities need to be monitored and validated



Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on an V2X traffic light

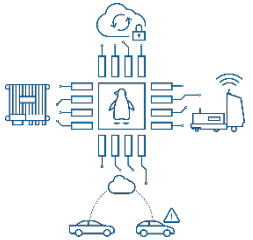




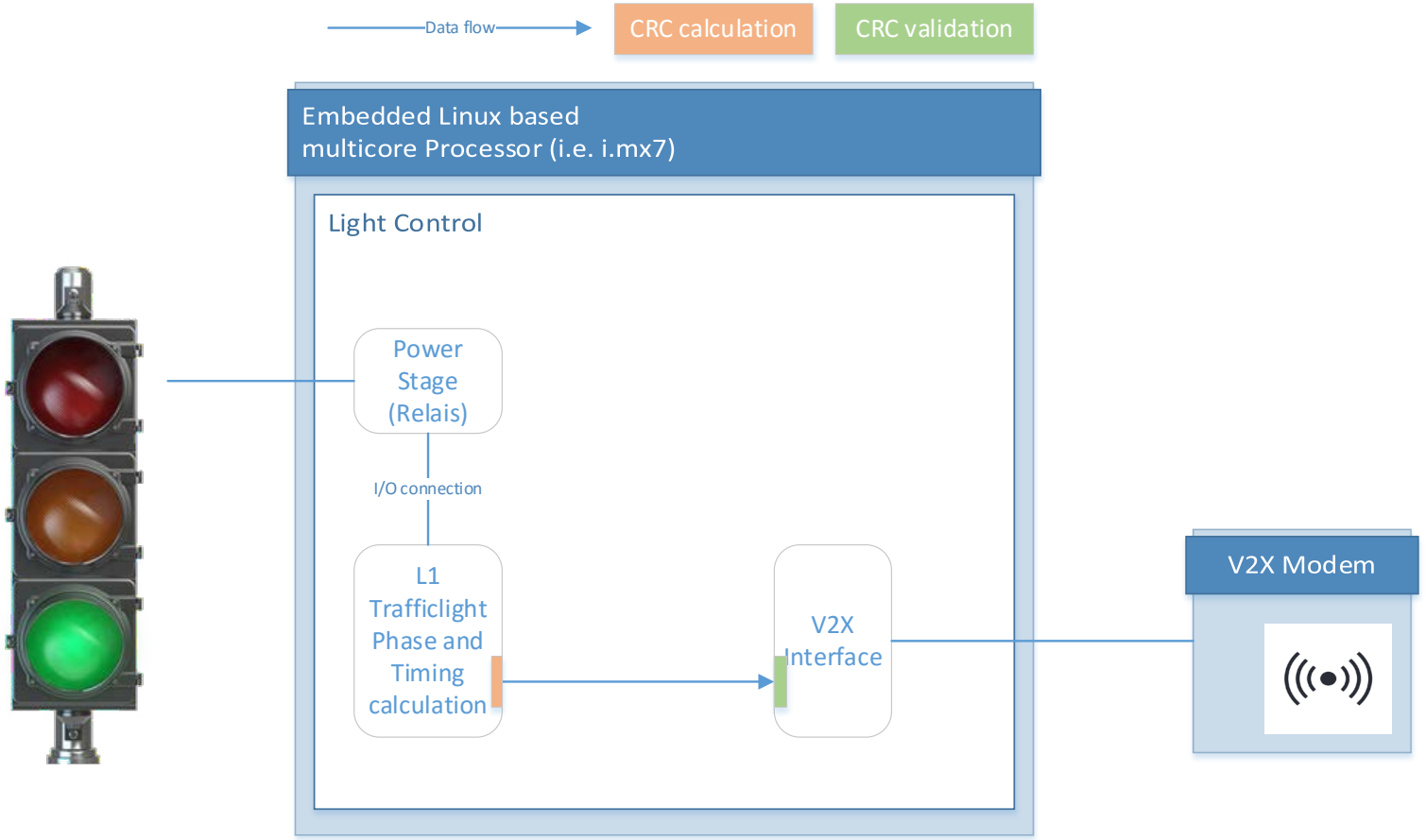
- Example
  - Data exchange between car and traffic light via radio (i.e. dedicated short range communication)
- Safety target:
  - Ensure data flow integrity
  - Ensure safe modes & conditions in driving situations
- Monitoring mechanisms
  - Checksum & message Counters
  - Cyclic Redundancy Checks
  - Keyed-Hash Message Authentication Code

Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on an V2X traffic light



Data Flow

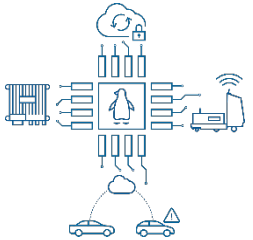


Bosch Engineering | Nico Peper, Jan-Christian Arnold, Hans-Leo Ross | October 2017

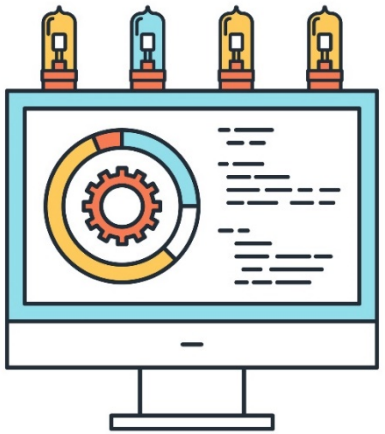
BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on an V2X traffic light



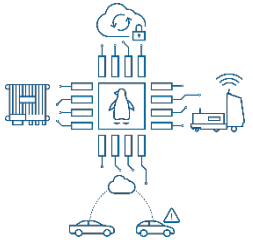
Data Processing

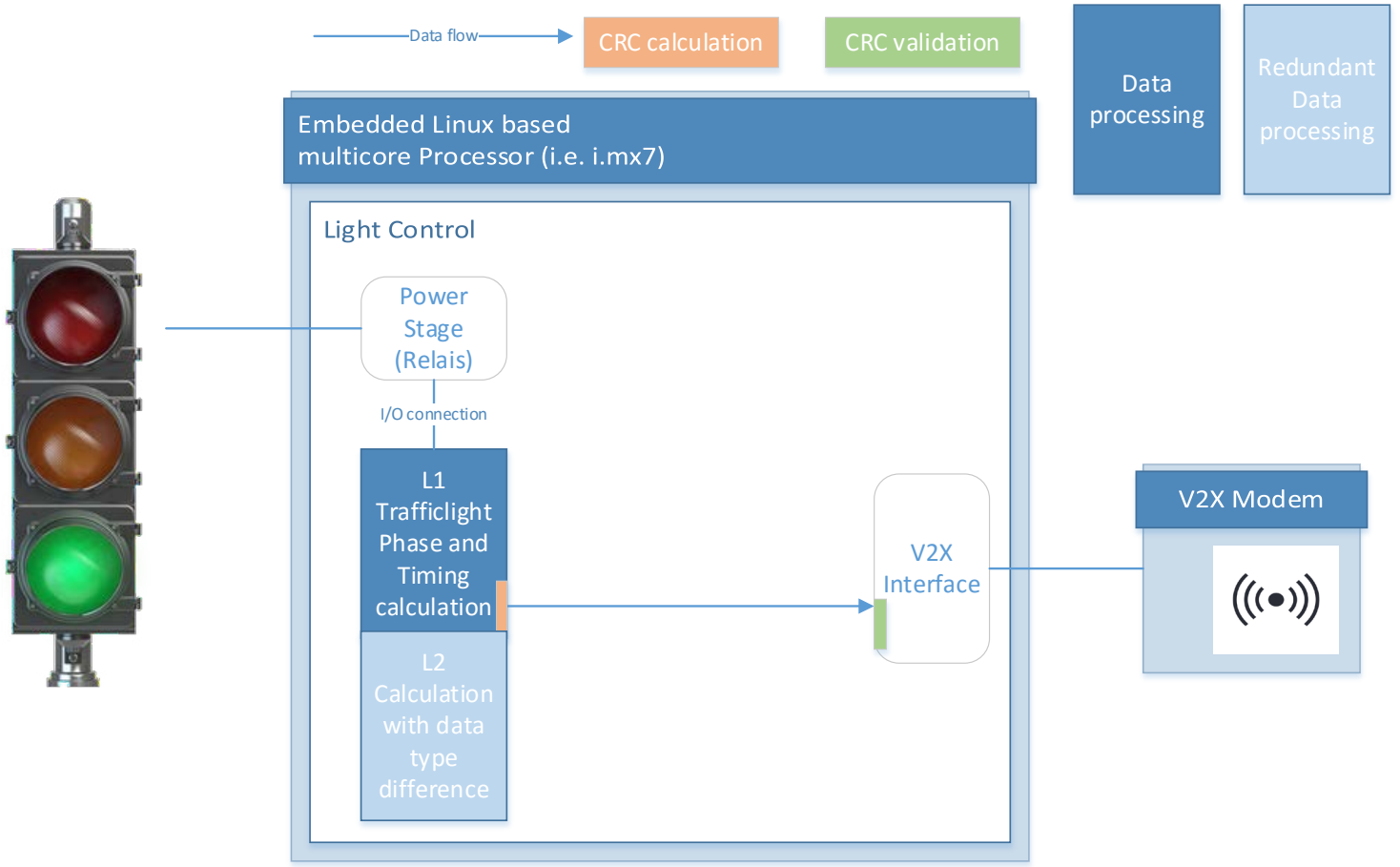


- Example
  - Process traffic light status for the V2X communication stream
- Safety target:
  - Ensure data integrity by avoiding calculation based errors, i.e.:
    - bit errors
    - rounding or overflow errors
- Monitoring of data processing
  - Redundant calculation including diverse calculation based on different data structures / types etc.

Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on an V2X traffic light





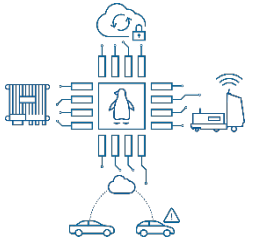
Data Processing

Bosch Engineering | Nico Peper, Jan-Christian Arnold, Hans-Leo Ross | October 2017

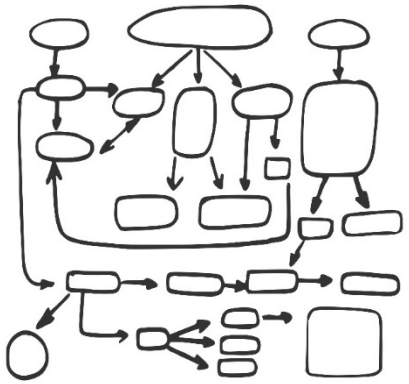
BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on an V2X traffic light



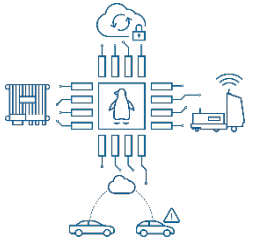
Data / System Control

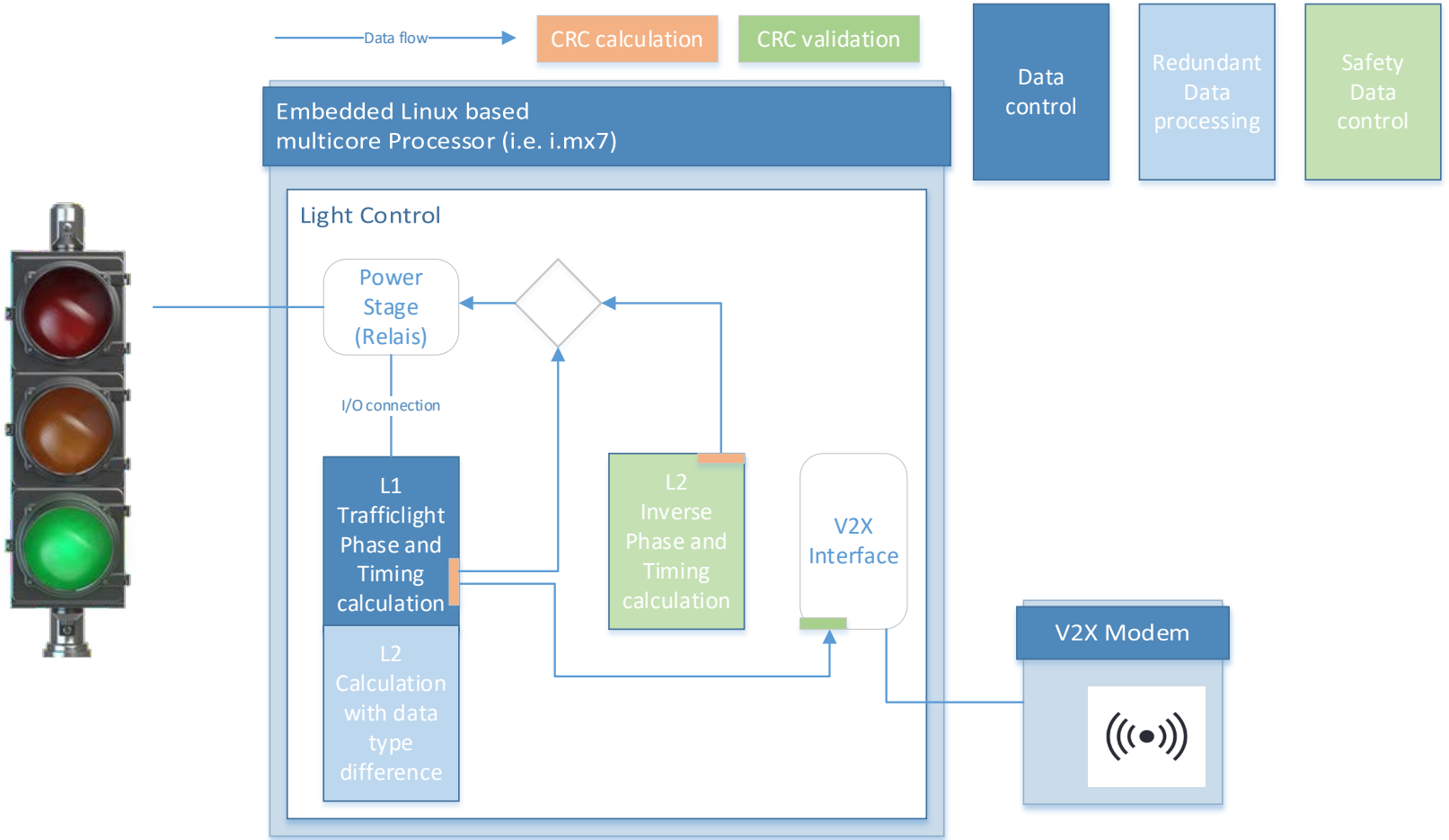


- Example
  - Operating traffic light colours and status (i.e. system control state machine)
- Safety target
  - System control integrity is ensured
- Monitoring
  - Monitoring of forbidden states

Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on an V2X traffic light



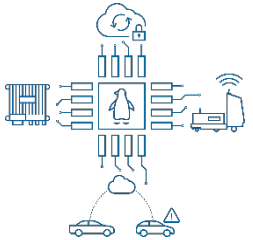


Data / System Control

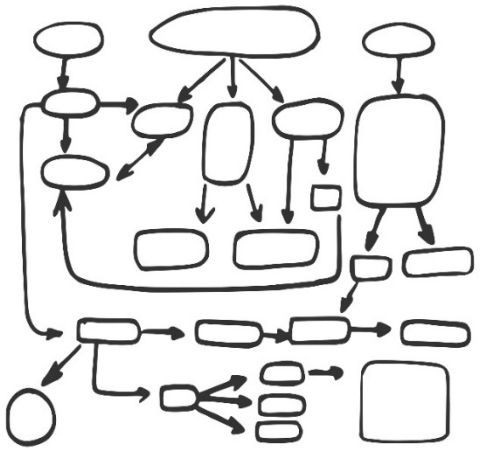
BOSCH

Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on an V2X traffic light



System Control (real time integrity)

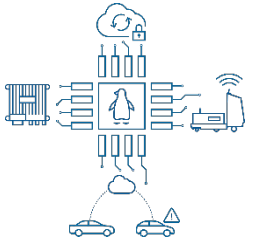


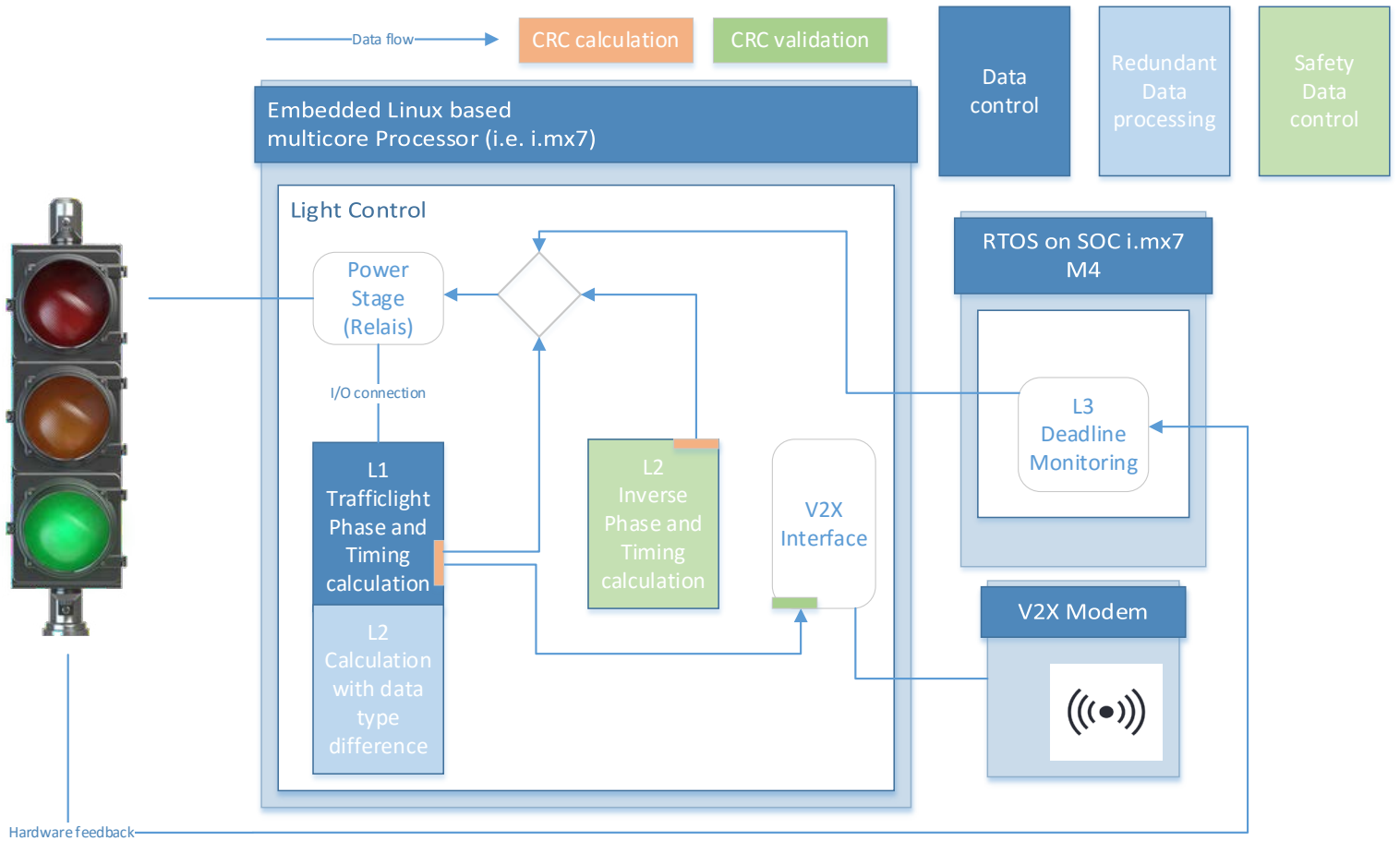
- Example
  - Ensure correct real time behaviour of the traffic light
- Safety target
  - Traffic lights are operated conforming the real system state
- Monitoring
  - A safely operated entity is needed to ensure the system operation and the traffic light feedback (deadline monitoring)

Bosch Engineering | Nico Peper, Jan-Christian Arnold, Hans-Leo Ross | October 2017

Open Sesame! Functional Safety for Linux in Automotive

Implementing ASIL B on an V2X traffic light



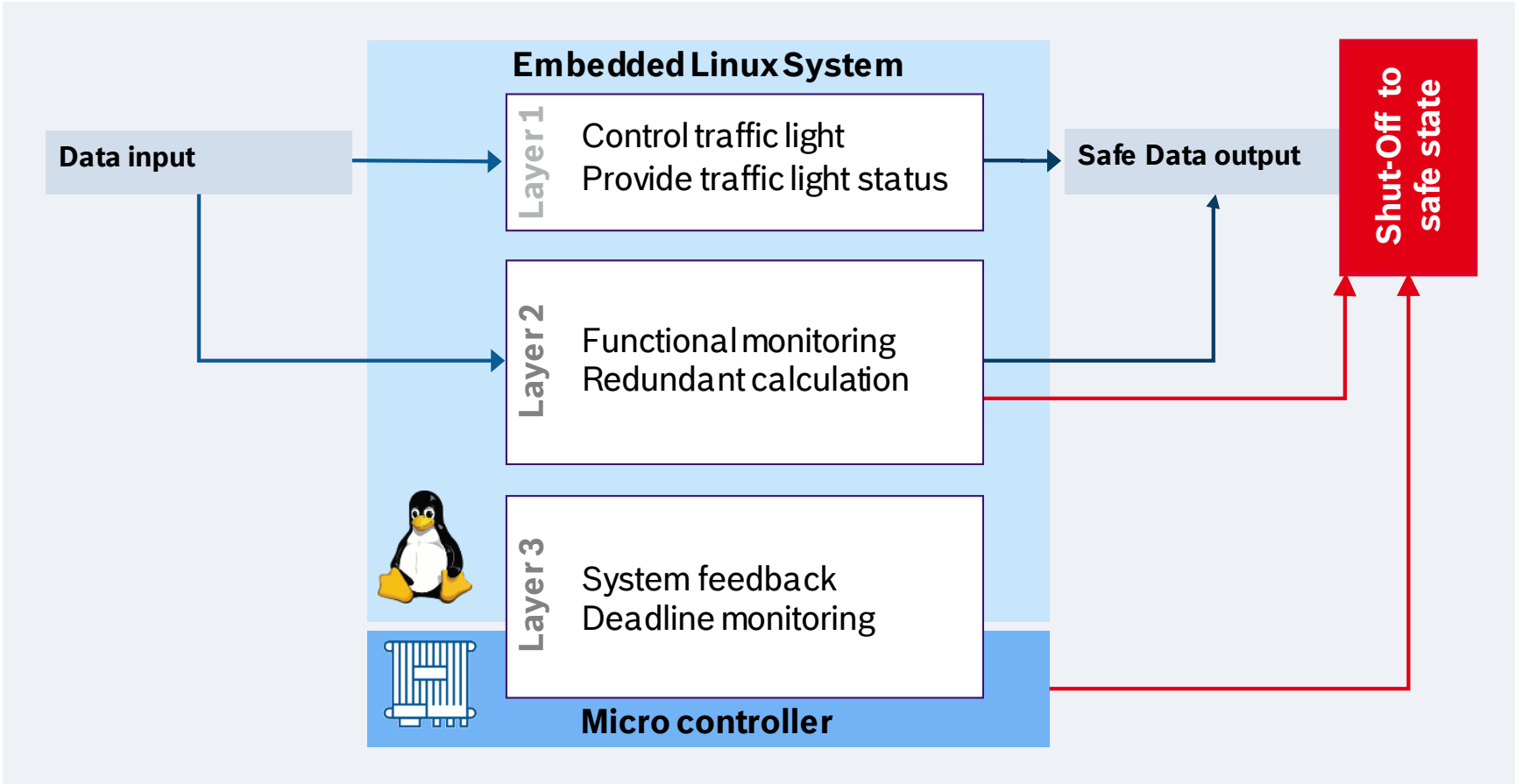


System Control (real time integrity)

BOSCH

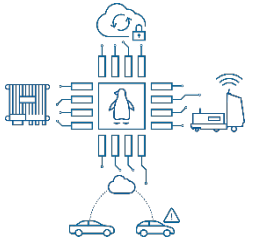
Open Sesame! Functional Safety for Linux in Automotive

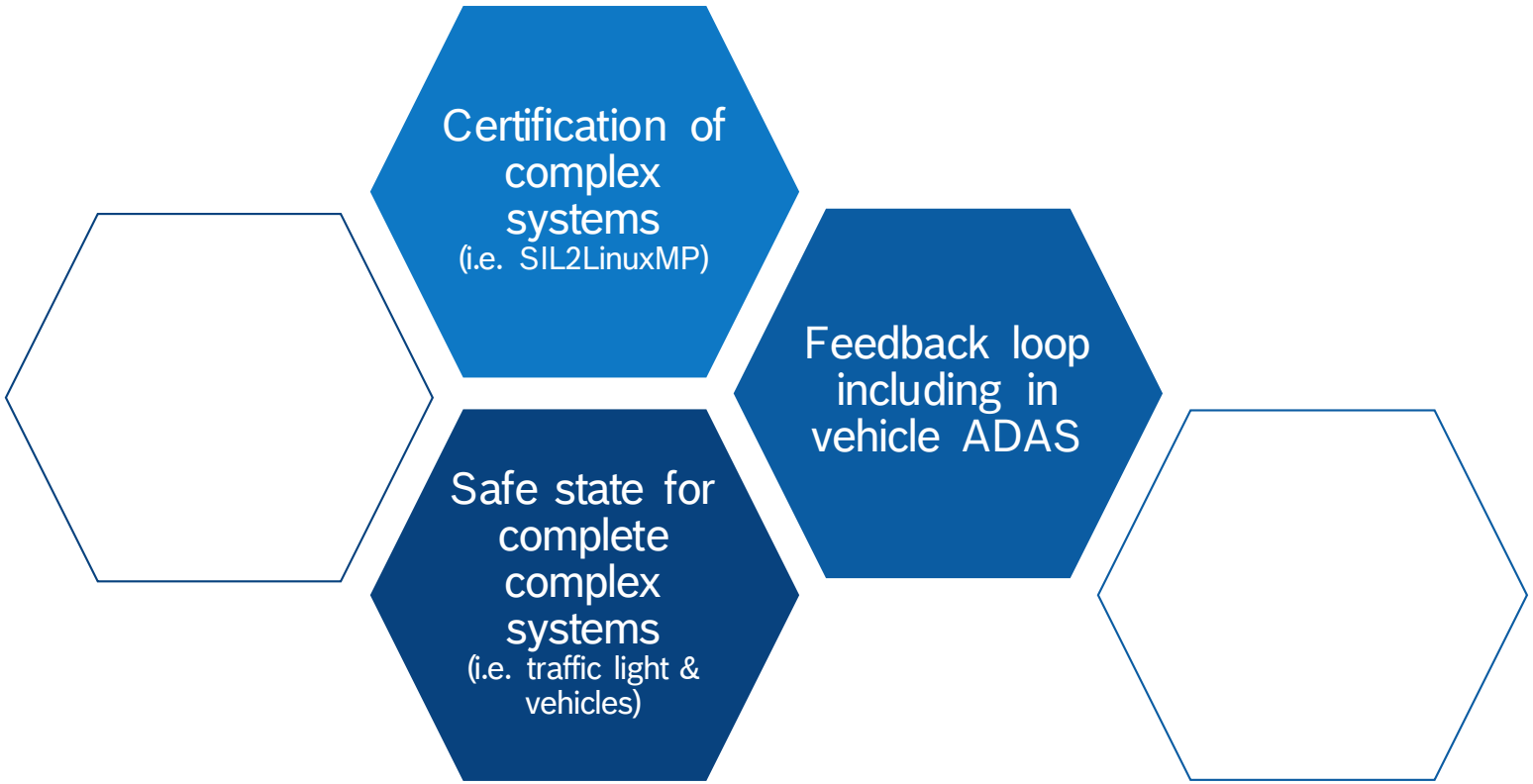
Implementing ASIL B on an V2X traffic light



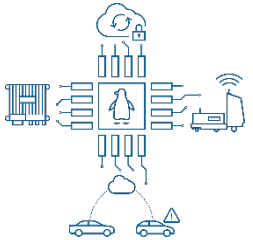
Open Sesame! Functional Safety for Linux in Automotive

Safety Relevant Open Questions in a V2X Context





Open Sesame! Functional Safety for Linux in Automotive
Conclusion



- Embedded Linux is making a clear push to automotive core systems

- Presented challenges concerning embedded Linux (i.e. licence obligations, real time behaviour and ASIL conformity) can be tackled

- By introducing the functional view to system safety Linux isn't a blocking point for functional safety

- The three layered safety concept is proven in use in various product families and can be fully applied to embedded Linux systems

- Challenges exist! They still need to be solved
  - This should be a shared effort of the automotive industry and the Linux community

Open Sesame! Functional Safety for Linux in Automotive

Contact

Nico Peper

Product line owner embedded Linux based IOT systems

+49 (151) 1680 5265
nico.peper@de.bosch.com

Jan-Christian Arnold

Expert embedded Linux based IOT systems

+49 (7062) 6357
jan-christian.arnold@de.bosch.com

Hans-Leo Ross

Senior Consultant Safety

+49 (173) 314 1579
hans-leo.ross@de.bosch.com


BOSCH
Parkhaus